「アクティブ・サイバー・ディフェンス」事始め
～攻撃者プロファイリングの意義について～

JPCERTコーディネーションセンター
早期警戒グループ マネージャ
脅威アナリスト
佐々木 勇人

本発表の問題意識

■ 現状（2022年11月 本発表の応募時点）

・安全保障3文書改訂に向けた検討が政府で進む中で、「積極的サイバー 防御（アクティブ・サイバー・ディフェンス）」がコンセプトに挙げられる

・「反撃」まで含むのか、含まないのか、などが話題になる中、その「定義」やどういうオペレーションがあるのか、またメリット／デメリットについて具体的な説明がどこからも出てこない

実はそんな用語の定義なんてないし、具体的な理論は誰も知らない！！

■ 問題意識

・（一般論として、この手の問題では）新たに検討される様々な「手段」が自己目的化する恐れがある

・（これも一般論として）「誰がそれをやるのか」議論が先行することで、本質的に手段を誤る恐れがある

・既存のインシデント対応現場との「乖離」や「衝突」が起きないか

具体的なオペレーションやどの脅威に対してどのような対抗手段を取るのか判断するためには、アナリストによる攻撃者の「プロファイリング」（※）が重要に

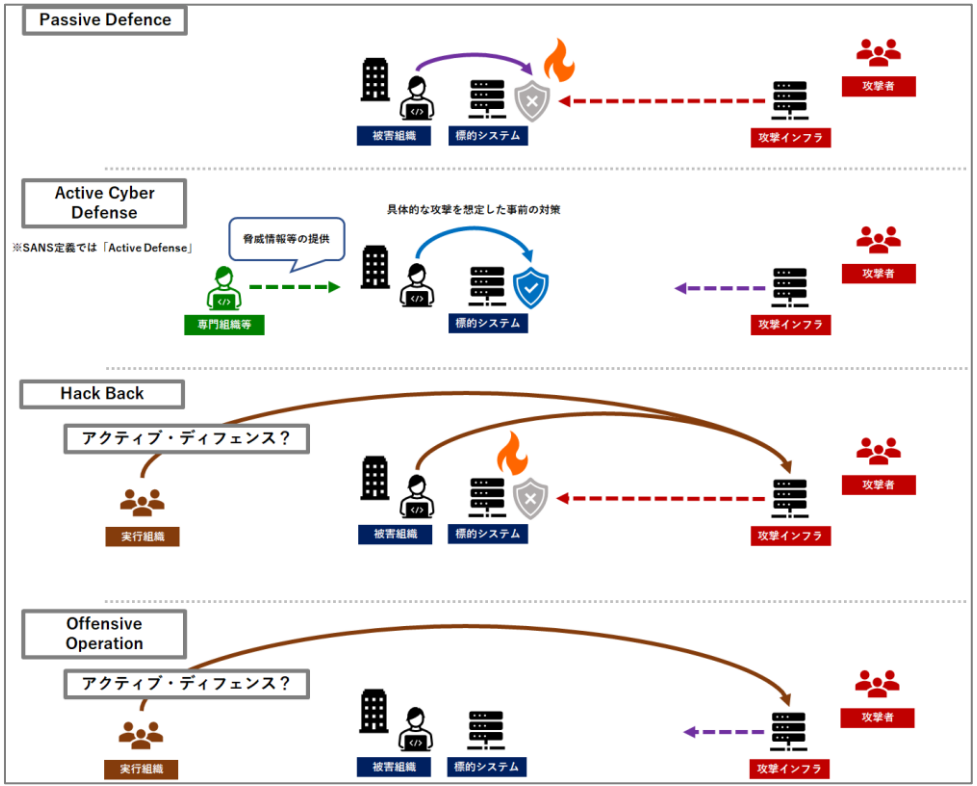
※犯罪の類型や犯行の特徴から犯人を推測する「犯罪プロファイリング」が有名ですが、本発表では、攻撃者のグルーピングや攻撃の特徴や傾向について分析することとして使います。

先行調査

- 2022年9月21日 JPCERT/CCブログ
- 「アクティブ・サイバー・ディフェンス」という用語が使われ始めた経緯や変遷、用語の“定義”のブレについて解説
- プロアクティブなサイバー攻撃への対抗手段として、様々な選択肢の組み合わせがあることを指摘

https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

先行調査から：用語の変遷について



【仮説】

様々な主体が用語を使う中で、サイバーセキュリティ以外の業界から流入した用語がミックスされたことで、概念が混乱／多様化してしまったのではないか

【背景の推測】

- 用語を用いた関係者がその時々に、より「ポジティブに聞こえる表現」を使っていたこと

  例：防御的な戦闘ドクトリン → 「アクティブ・ディフェンス」（1976年）

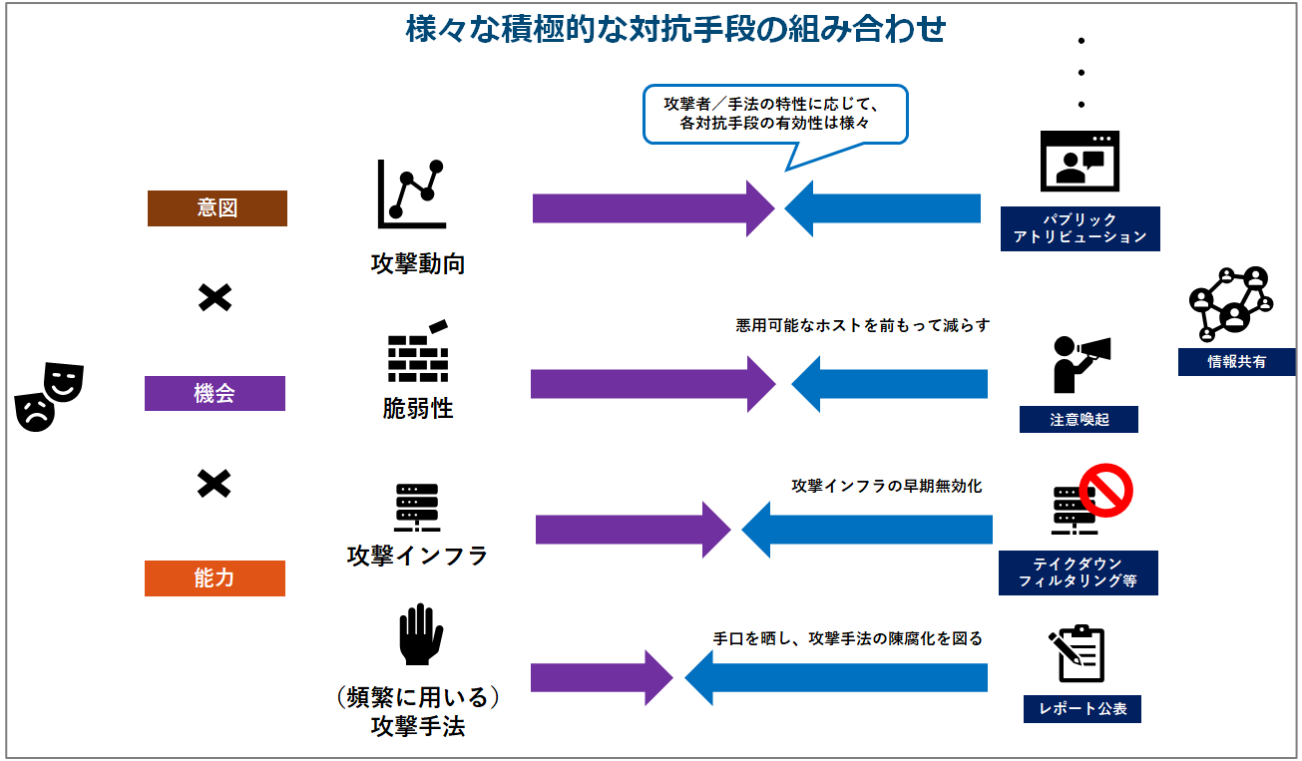
- 軍／インテリジェンス業界からサイバーセキュリティ業界への用語の「輸入」がなされたこと

  例：キルチェーン、スレットインテリジェンス、等々

https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

先行調査から：プロアクティブな対抗手段の選択肢

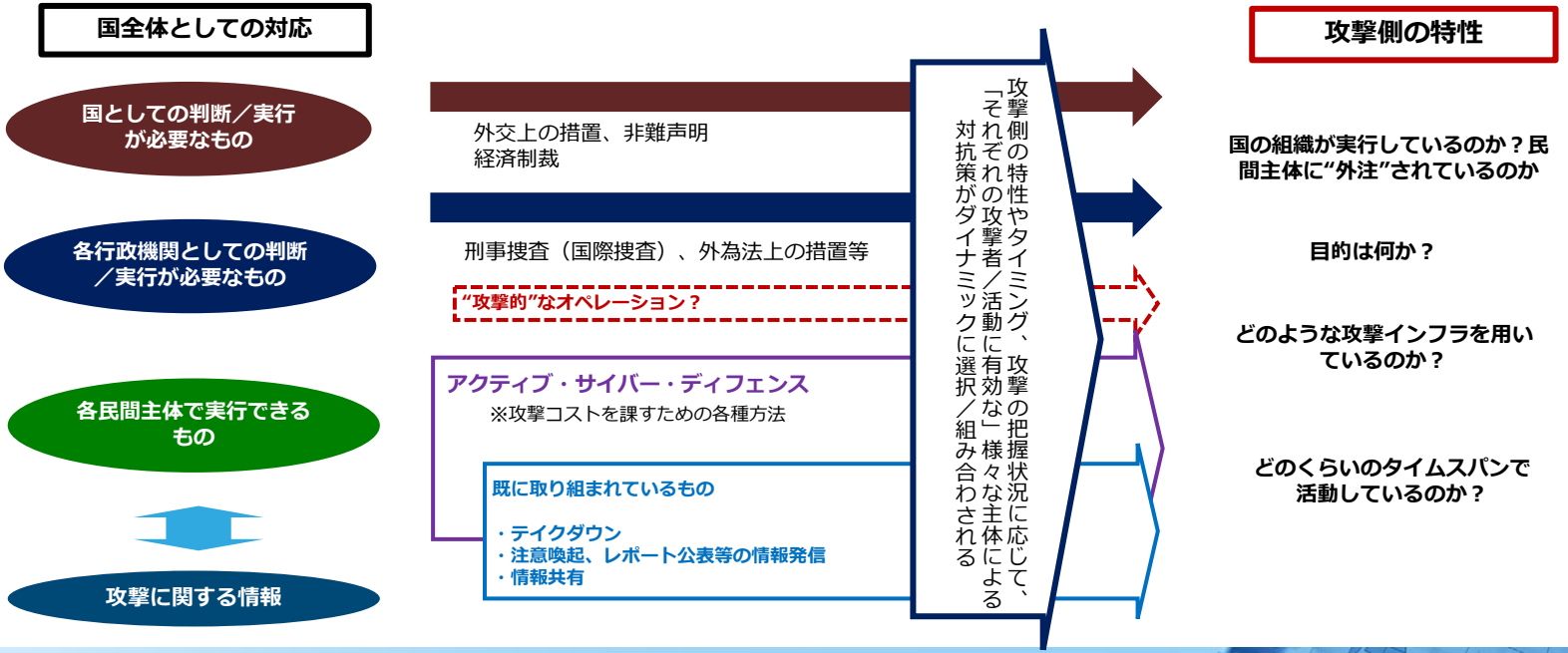
- プロアクティブな対抗手段は、攻撃的な手法以外に様々存在している



https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

より柔軟でダイナミックな対抗措置の検討へ

- 攻撃側への様々な対処オプションのうち、「アクティブ・サイバー・ディフェンス」や“攻撃的”なオペレーションというのはごく一部に過ぎず、攻撃側の特性に応じて機動的に対処オプションの選択が必要。
- とはいえ、「アクティブ・サイバー・ディフェンス」を検討していく中で、**「いままでやれていなかったこと」に挑戦していくことは有用ではないか？**



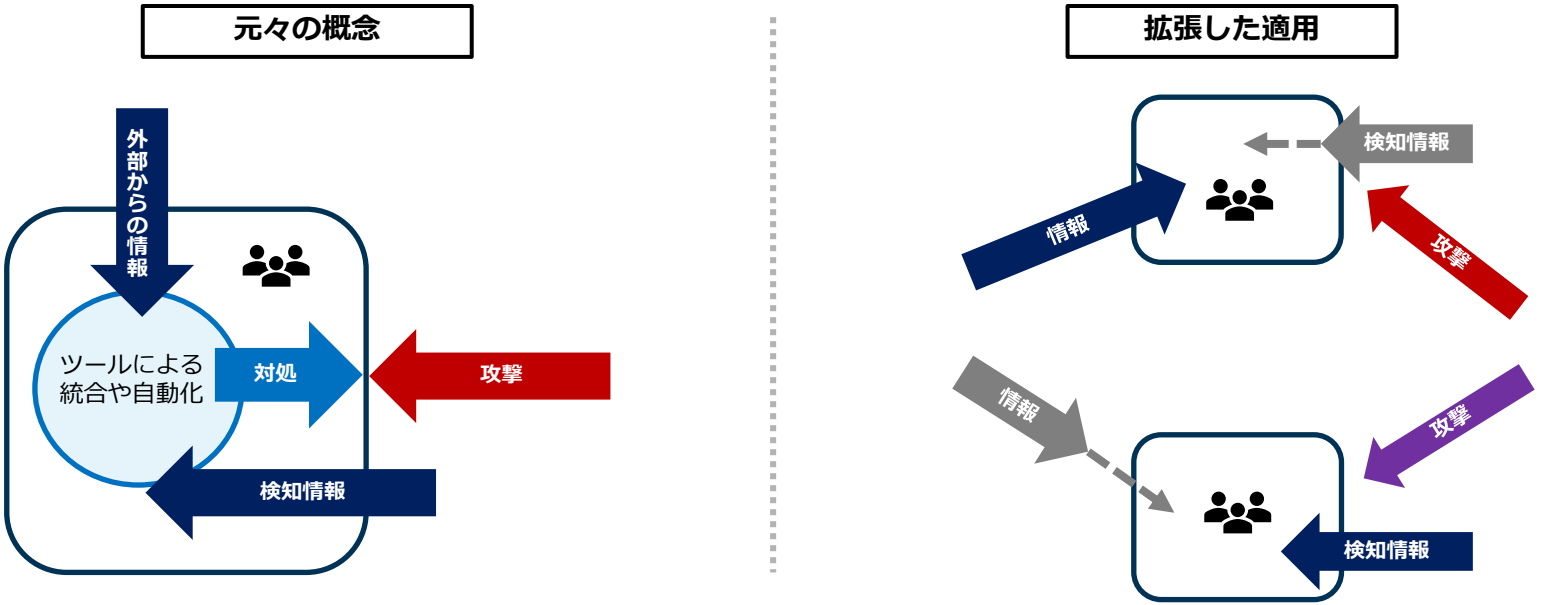
・・・でも結局、具体的なことがわからない

- 個別の事案対応の話なのか、国全体の話なのか
- 攻撃される前に対応することなのか、攻撃されてから対応することなのか
- 攻撃活動を停止させることなのか、妨害することなのか

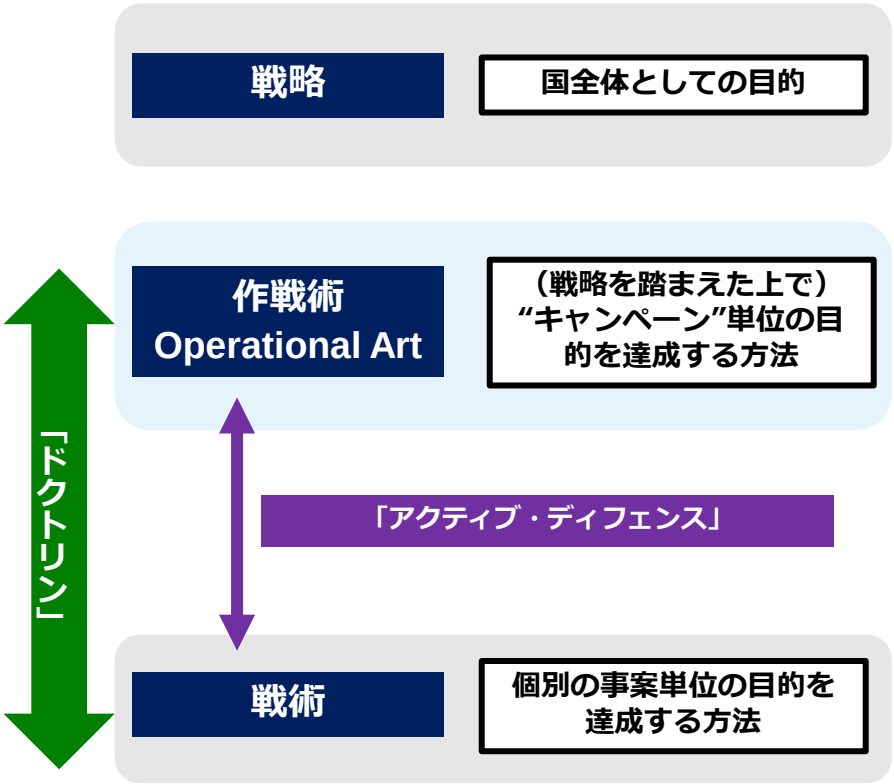
面倒ですが、もう少しだけ言葉の「定義」を振り返ります

元の「アクティブサイバーディフェンス」を拡大適用することの限界

- 元々は個別の組織単位での実施を想定した、プロアクティブな攻撃対処のコンセプト
- 業種／分野別、地域別で連携する場合、スケールが大きくなるほど組織間連携は困難になり、また、それぞれ受ける攻撃類型も異なるため、理屈通りのプロアクティブな対処は難しい



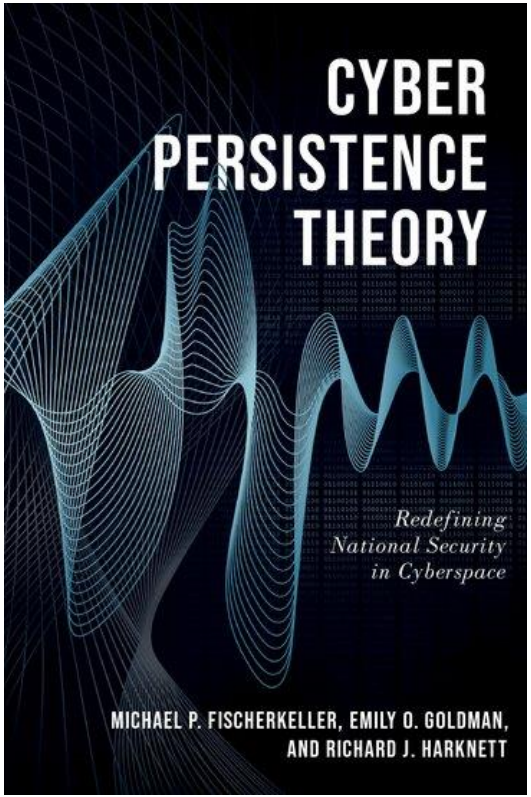
「アクティブ・サイバー・ディフェンス」のあいまいさの起源



- アメリカ陸軍戦闘教義FM100-5（1976年版）に登場する「**アクティブ・ディフェンス**」のコンセプト
- 作戦術（Operational Art）
  - 作戦術は戦役の術（”operational art is the art of **campaign**” （John English, 1996））
  - 作戦術は戦術的成功と戦略的達成点との間をつなぐもの（英統合ドクトリン）
- 「アクティブ・でフェンス」の概念は戦術レベルに焦点が置かれているとの批判があり、その後、作戦レベルでの克服に向けた改訂が行われていく
- 元々、“戦術”レベルである「アクティブ（・サイバー・）ディフェンス」を“作戦”レベルに拡張適用するための改良が必要

参考文献： 北川敬三「軍事組織の知的イノベーション ドクトリンと作戦術の想像力」、デイヴィッド・M・グランツ「ソ連軍 <作戦術> 縦深会戦の追及」 ほか

定義を考えるポイント：「キャンペーン」への注目

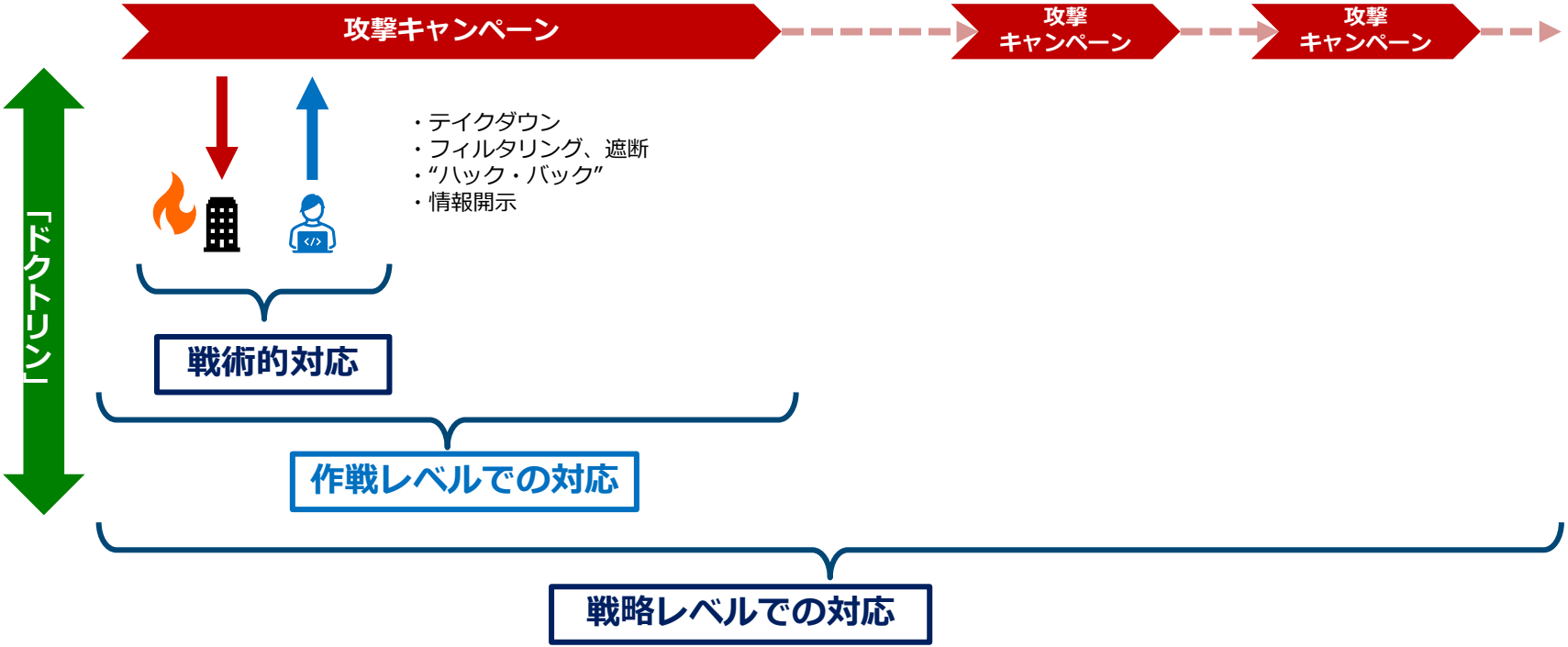


https://global.oup.com/academic/product/cyber-persistence-theory-9780197638255?cc=us&lang=en&

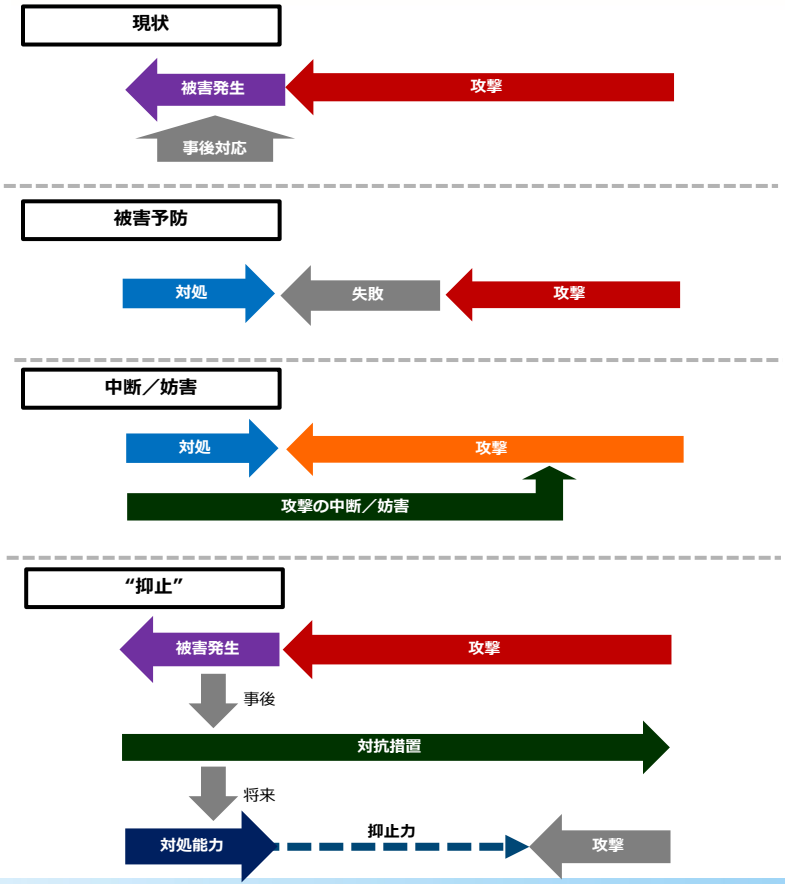
- Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett, “CYBER PERSITENCE THEORY”, 2022
- 国家主体を背景としたサイバー攻撃のほとんどが、「強制：coercion」ではなく、「搾取：exploitation」であり、既成事実化（fait accompli）であると指摘。
- 既存の抑止理論をベースとしたパブリックアトリビューションなどの対抗措置に効果がなかった点など、これまでの米国に対抗手段実施の歴史を評価・分析。
- 攻撃「**キャンペーン**」単位に注目し、これに対して、持続的な「Direct Cyber Engagement（直接的なサイバー行動）」による、優位性維持のためのアプローチである「Cyber Persistence Theory」を提言

ドクトリンとしての「アクティブ・サイバー・ディフェンス」

- 「縦軸：何に対して、何をするのか」に対して、キャンペーン単位における「横軸：何を目的としていつやるのか」が必要になる



定義を考えるポイント：「タイミング」と「コスト」



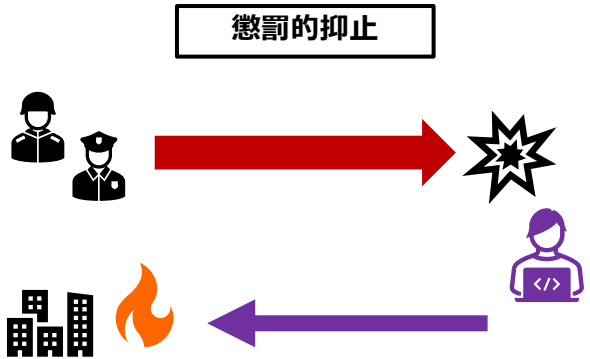
- 目的が「被害予防」だとした場合、どのタイミングで、どのような攻撃「被害」を防ぐことなのか
  - — APT攻撃を早期に捕捉することは困難。最初に“被弾”した組織からの情報が必要
  - — 例えば、不正アクセスを受けてしまったが、これを早期に捕捉した後、情報漏えい被害前に攻撃を停止させることも「被害予防」なのではないか？

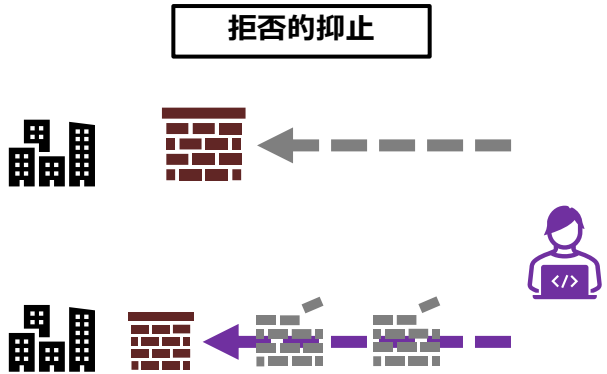
- 攻撃側に「コストを課す」ということ
  - — 攻撃着手／成功させるためのコストを上げること（拒否的抑止？）
  - — 攻撃を中断させること（これも拒否的抑止？）
  - — （事後の）懲罰的抑止としての制裁措置

攻撃者に「コストを課す」とはどういうことか

- 欧米各国政府等が使うことが増えた「（攻撃者に）コストを課す（imposing costs）」という用語
- ダブルミーニングになっているのではないか

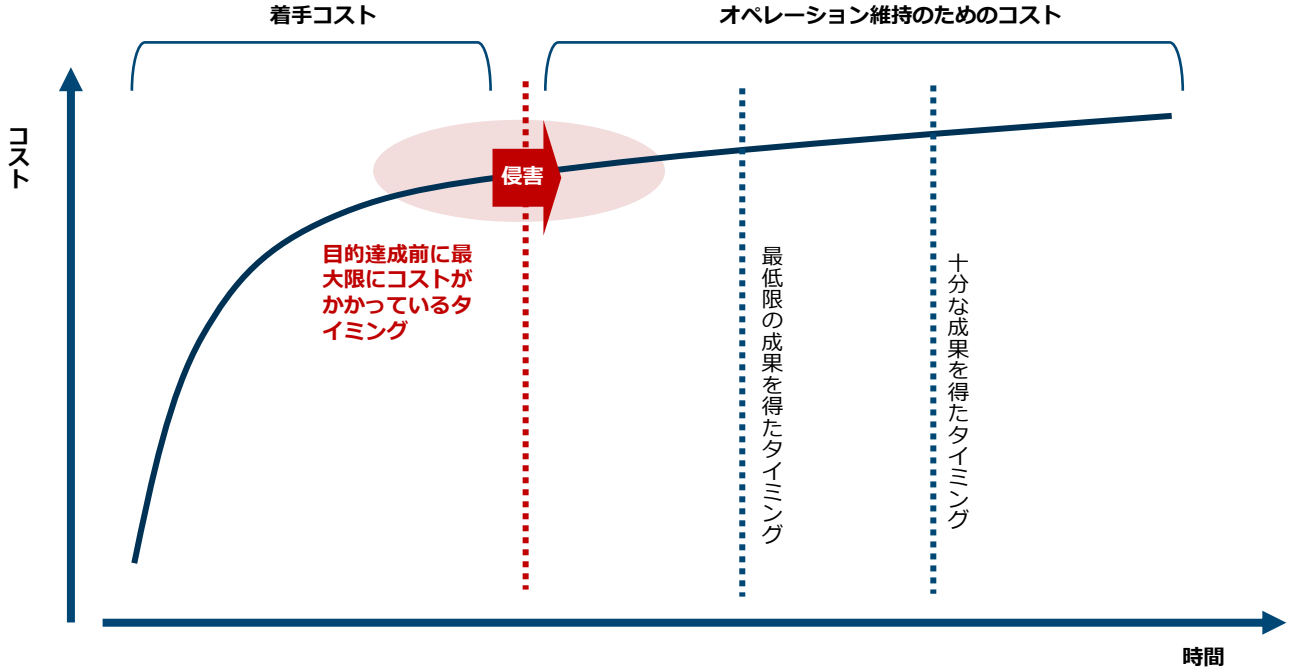
- 「懲罰的抑止」的な文脈：「代償を払わせる」意味での「コスト」。あくまで、攻撃後の措置により、その後の抑止を狙うもの。
- 「拒否的抑止」的な文脈：攻撃が成功しづらい／成功させるために多大な負担が必要という意味での「コスト」。





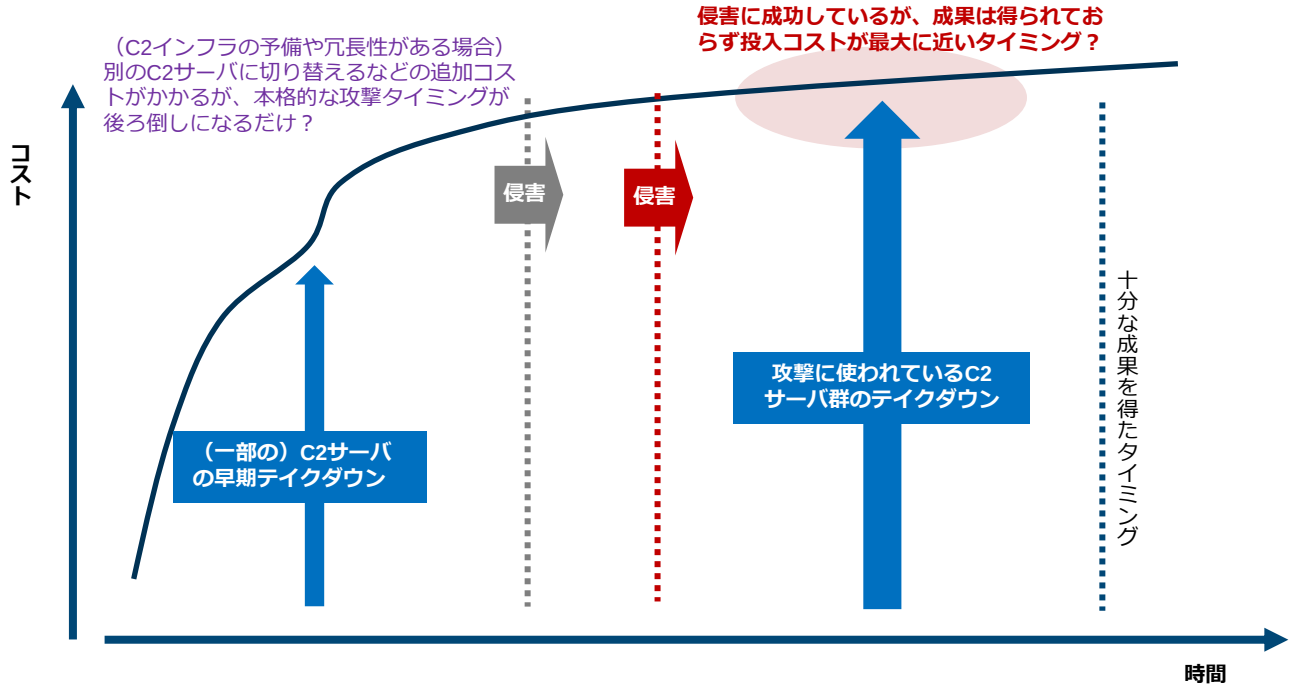
攻撃者のコストを再考する

- 人的リソースの準備、マルウェア開発、攻撃インフラの準備、標的の選定、初期侵入経路の開拓、など、標的組織への侵害直前までが最もコストがかかるフェーズなのではないか？
- 「コストを課す」だけでなく、攻撃者側の逸失利益やサンクコストを発生させる／増やす、というアプローチもありうるのではないか？



攻撃者のコストを再考する

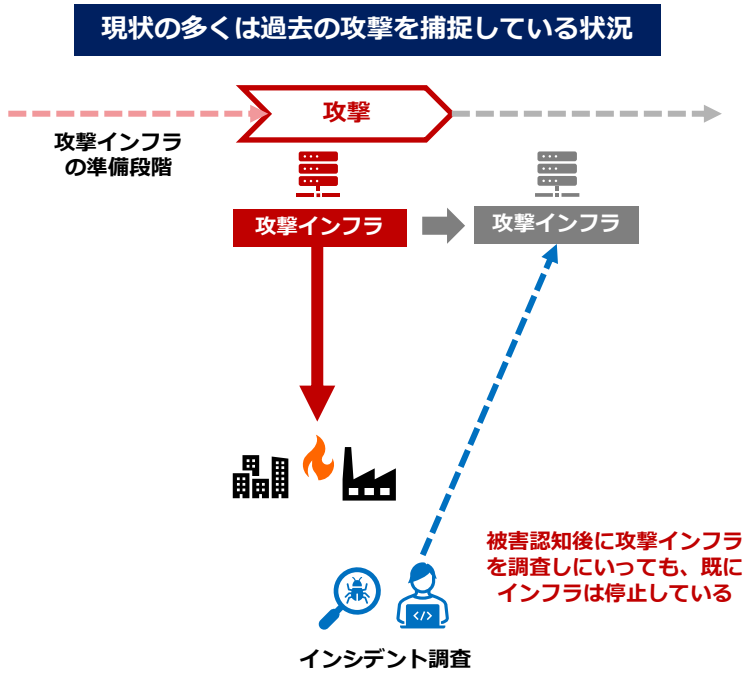
- 本格的な攻撃活動前のC2サーバ群の一部を捕捉してテイクダウンすることよりも、攻撃は始まってしまったが、C2サーバ群を概ね捕捉でき、かつ、攻撃者側のサンクコストが最大であるタイミングで攻撃を中断させることの方がより多くの「コストを課す」ことができるのではないか？
- **攻撃者の的確なプロファイリングが必須**である

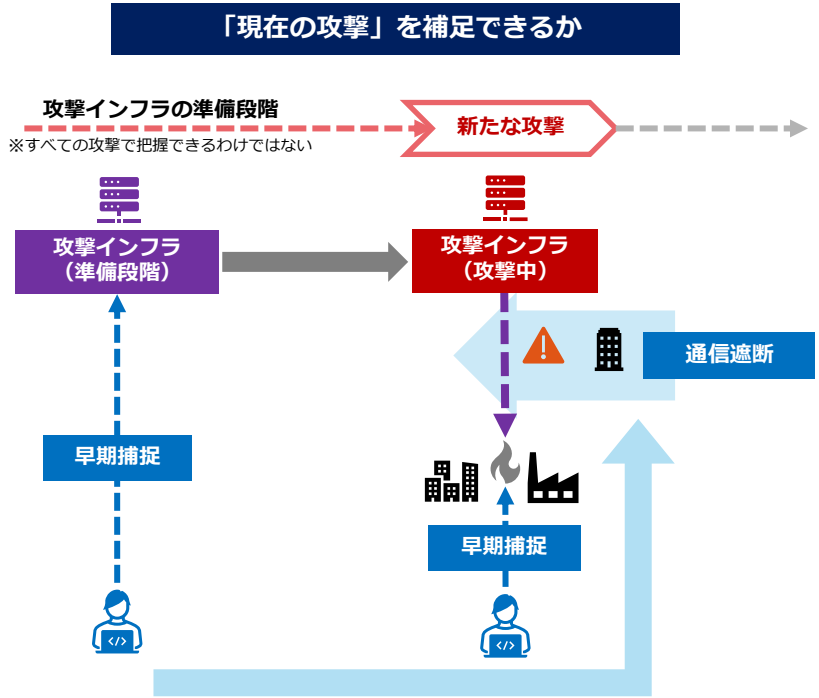


個別の「戦術」について

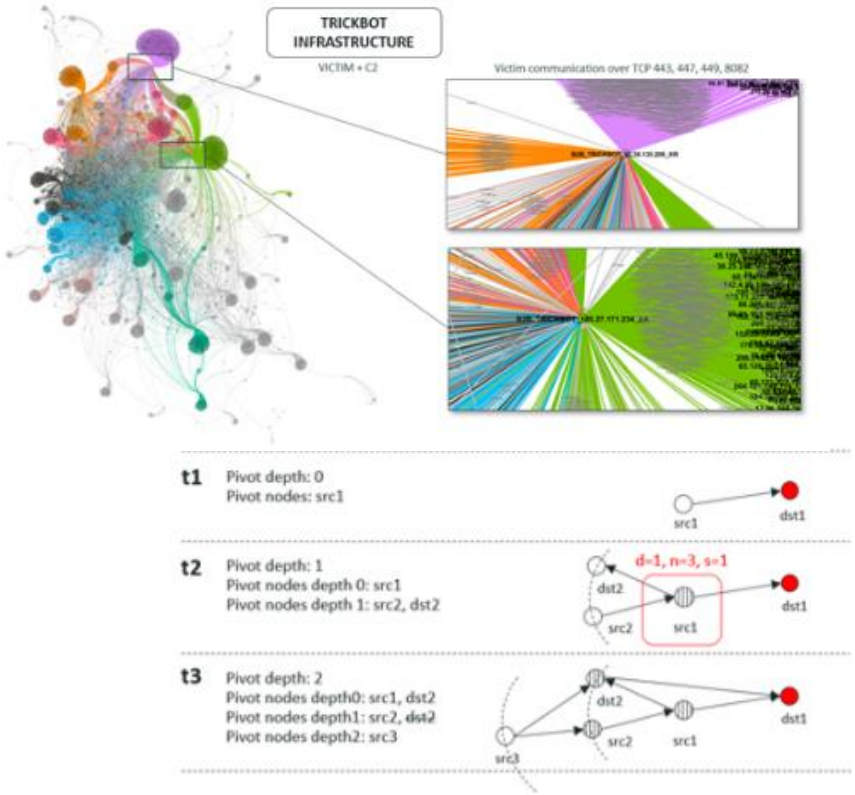
個別論点：通信遮断

- 法的課題や技術的ハードルを仮にクリアできたとして、そもそも、不正通信元を早期に把握することが出来なければ、プロアクティブな措置にならない





攻撃インフラを積極的に探した例

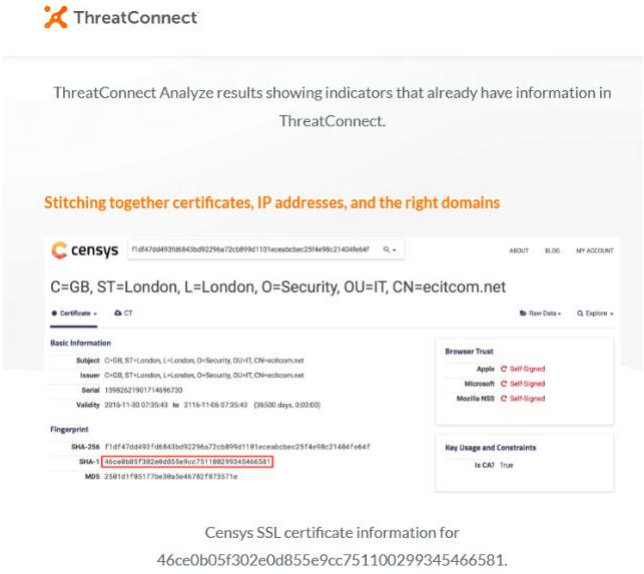


https://insight-jp.nttsecurity.com/post/102fvek/12-5-soc-trickbot

- Netflowデータ解析による、Trickbotの攻撃インフラ構成の調査
- ボットネットのネットワーク連関性の特徴から攻撃インフラを構成するC2サーバ構成を探し出す方法を検証
- ボットネットのインフラ構成・通信のパターンに一致する特徴を持つ通信をNetflowデータから抽出
- なお、Trickbot自体のテイクダウン（2020年10月）には「失敗」（※後ほど解説）している

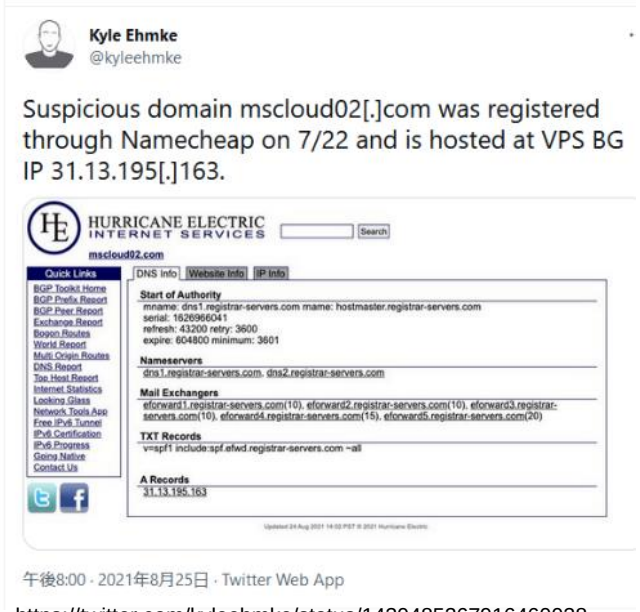
攻撃インフラを積極的に探すことはできるのか（C2ハンティング）

- ThreatConnectによる過去の調査
- APT28（Sofacy）のC2サーバでよく使われるSSL証明書の特徴から、既知以外のC2サーバを調査



https://threatconnect.com/blog/using-fancy-bear-ssl-certificate-information-to-identify-their-infrastructure/

- 攻撃者がよく使うレジストラ、ネームサーバ、取得時期、紐づいたIPアドレス／ホスティングサービス、の特徴から、疑わしいドメインを探し出す（※登録≒攻撃準備段階で捕捉する）。

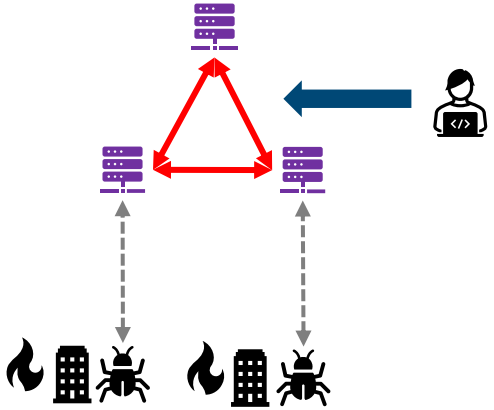


https://twitter.com/kyleehmke/status/1430485267916460038

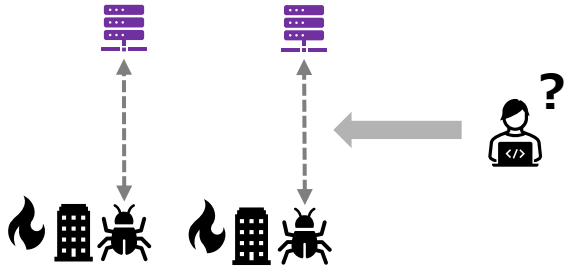
プロアクティブなC2探しはできるのか

- 2021年電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめと、これを受けた4団体ガイドラインの改定
  - — Net Flow情報を用いたC2の調査・特定を認める
  - — ワンストップに即応的な遮断まで現時点では想定されていない
- NetFlow情報の場合、ボットネットのような、C2間で特徴的な相互通信を行う攻撃インフラを探すことはできるが、単独で存在するC2サーバを探すことはできない。

既知のインフラ構成の特徴から探し出す



単独の攻撃インフラをどう探すのか



通信遮断の効果に係る評価

※主に、APTへの対抗を想定した場合

■ 他の対抗措置との比較した際の優位性
- 被害発生前に実行可能
- 被害組織側の対応コスト負担が少ない
- 攻撃者側のコストが最大限のタイミングで対抗できる

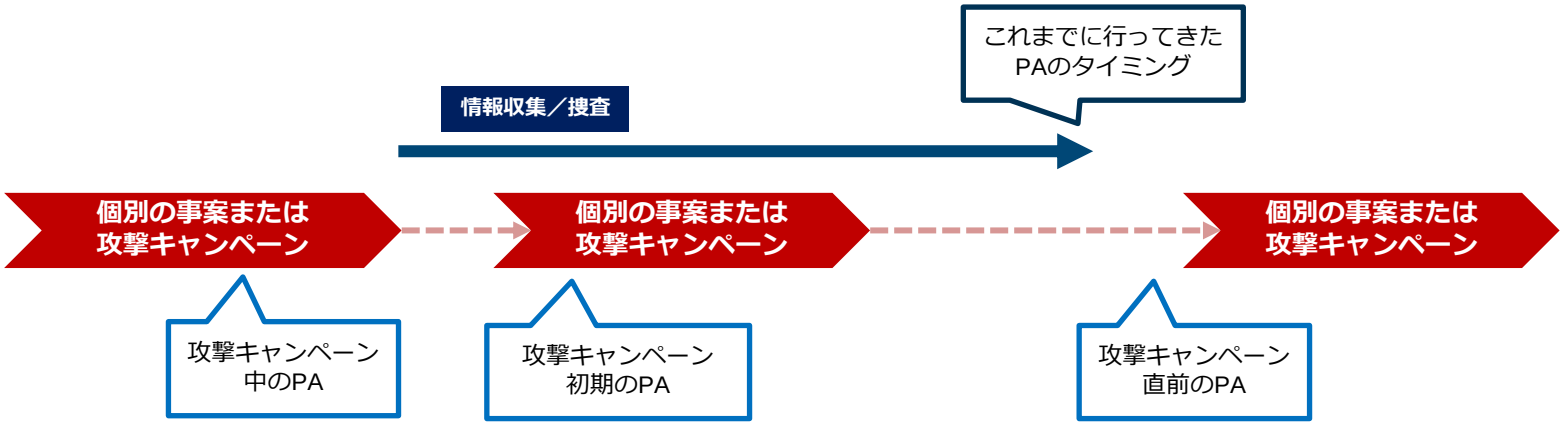
■ 対抗措置としての効果の限界
- 既知の攻撃者／インフラに関する情報の蓄積がある程度存在する攻撃活動に対して実行可能（例：稼働してしばらく経過している大規模なボットネット）
- 遮断後、別のC2サーバに切り替えられる可能性
- その他、通信遮断前提での冗長性対策を打たれる恐れ
- いたちごっこになる恐れ（通信事業者側の負担が継続的に増える）

■ 課題
- NetFlow情報だけで捕捉できる攻撃通信は限定的
- 被害現場で観測された攻撃インフラだけでなく、攻撃グループ毎の攻撃インフラの特徴から、未確認の攻撃インフラを網羅的に捕捉することが必要

⇒攻撃者のプロファイリングが重要

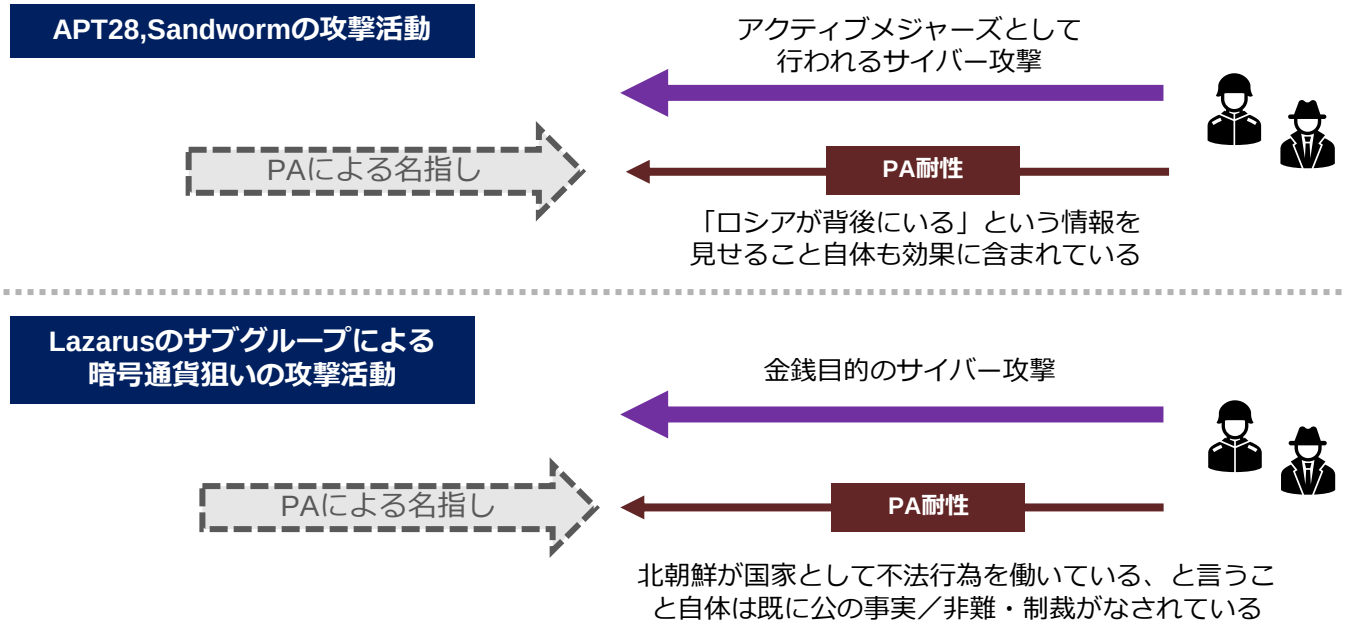
個別論点：「パブリックアトリビューション」問題

- 「オーディエンス」が誰なのかによって、パブリックアトリビューション（PA）の内容、粒度、タイミングは変わる
  - ― 攻撃者への牽制なのか
  - ― 背景主体への牽制／メッセージなのか
  - ― 注意喚起目的なのか
  - ― 同盟国との関係性においてなのか
  - ― 国際社会への訴えのためか



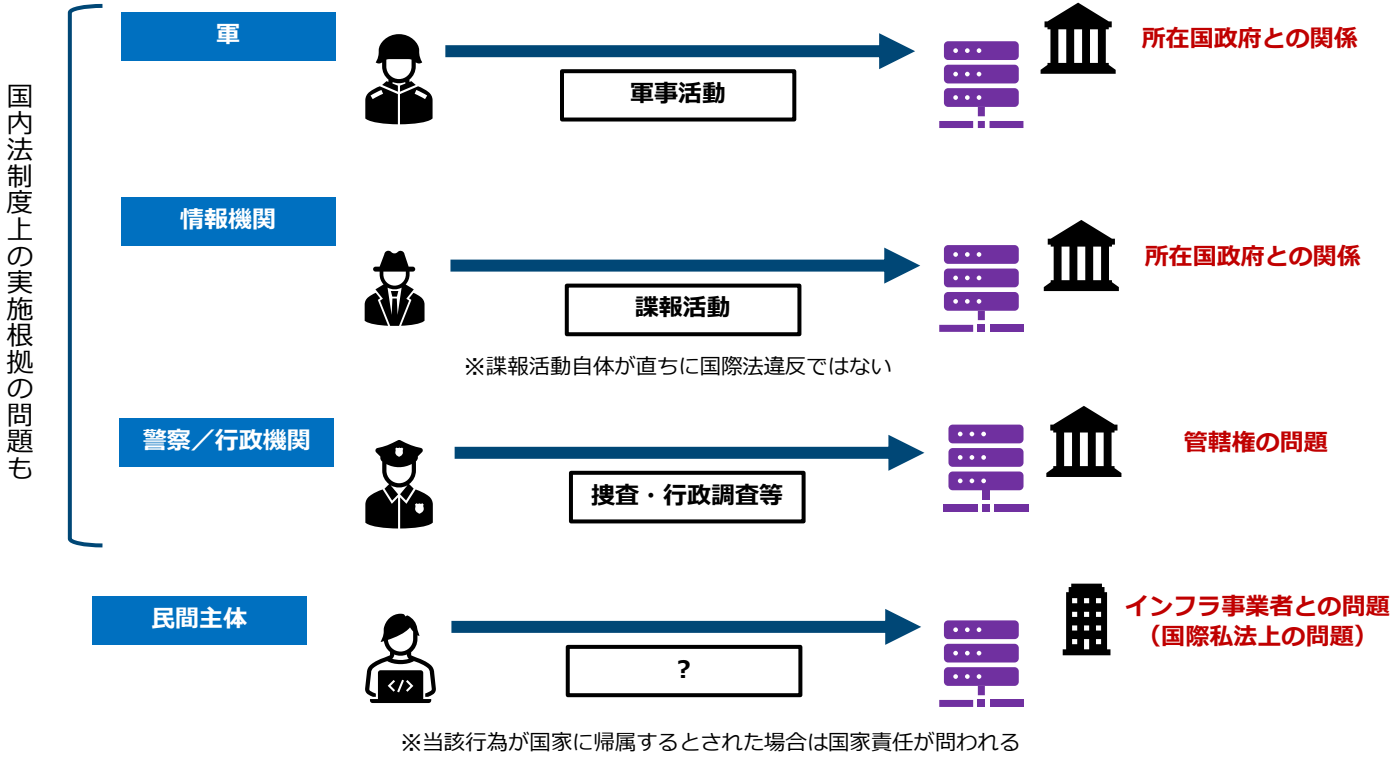
パブリックアトリビューション「耐性」の問題

- 「“パブリックアトリビューション“神話」について
- 対抗措置＝パブリックアトリビューションという論が出てきがちだが、アトリビューション「耐性」が強い攻撃活動／グループが多く存在している
- **攻撃者の的確なプロファイリングが重要**



個別論点：“積極的”越境アクセス ― 誰がやるのか―

- 目的だけでなく、実行主体によって同じアクセスでも法的性質が変わってしまう



ケーススタディ：BlackTechのC2サーバ調査

C2サーバーのコントロールパネル

調査の過程で、Gh0stTimesのコントロールパネルの存在を確認しました。図8は、コントロールパネル起動時のGUIです。確認したコントロールパネルは「Times v1.2」という名前が付けられていました。

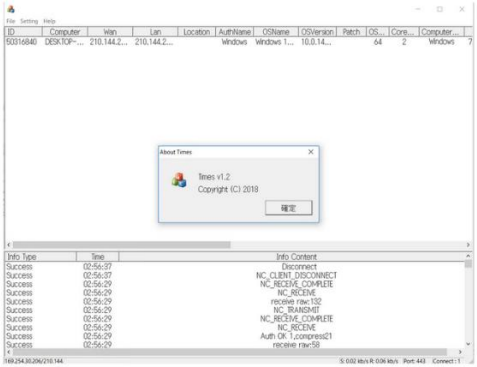


図8：Gh0stTimesのコントロールパネル

- https://github.com/Yang0615777/PocList
- https://github.com/liuxu54898/CVE-2021-3019
- https://github.com/knownsec/pocsuite3
- Citrix exploit tool
- MikroTik exploit tool
- Exploit for CVE-2021-28482
- Exploit for CVE-2021-1472/CVE-2021-1473
- Exploit for CVE-2021-28149/CVE-2021-28152
- Exploit for CVE-2021-21975/CVE-2021-21983
- Exploit for CVE-2018-2628
- Exploit for CVE-2021-2135

- 2021年9月のJPCERT/CC分析ブログ
- 攻撃者側の攪乱目的や、調査者側への「罠」の可能性も想定された
- 攻撃インフラや攻撃者の「武器庫」、など、攻撃者により近い箇所から得られる情報は、攻撃者のプロファイリングの精度を高める

JPCERT/CC 攻撃グループBlackTechが使用するマルウェアGh0stTimes
https://blogs.jpcert.or.jp/ja/2021/09/gh0sttimes.html

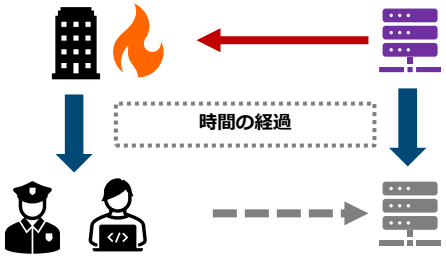
個別論点：“積極的”越境アクセス ―どこに「反撃」するのか？―

- 情報入手やタイミングの問題だけでなく、「反撃」先が基本的に（海外の）民間インフラである、ということが忘れられている

時間的制約で反撃「先」が見つからない問題

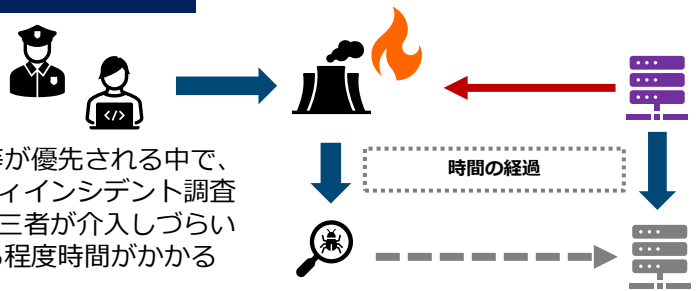
一般的な不正アクセス事案

・そもそも攻撃の認知が遅い（認知時点で攻撃が終了しているケースが多い）
・第三者の介入までが遅い（基本的に“後追い”している）



大規模サイバー事案

・復旧対応等が優先される中で、セキュリティインシデント調査のために第三者が介入しづらい
・調査にある程度時間がかかる



反撃「先」が妥当か問題

・攻撃インフラは基本的に民間インフラ（サーバ）上で稼働している
・不正契約によるものだとしても、反撃によりインフラ事業者自身や他の契約者に被害が出た場合の問題

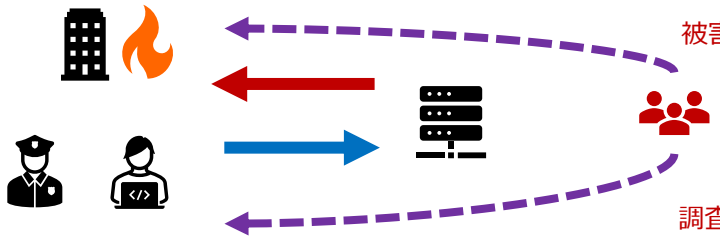
クラウド事業者
ホスティング事業者
ISP 等

個別論点：“積極的”越境アクセス ―「反撃」後に何が起こるのか？―

- 攻撃者毎における技術的／オペレーショナルに現実的な想定での議論が必要
- 特に、対抗措置に対する攻撃者側の対抗手段や「反撃」にどのように備えるのか予備知見がない

現在進行中の攻撃を認知できた場合

・テイクダウン／差止のほか、直接的操作によりC2サーバを停止させる
・攻撃者側に何らかのサイバー攻撃を行う



攻撃側はどう出るか

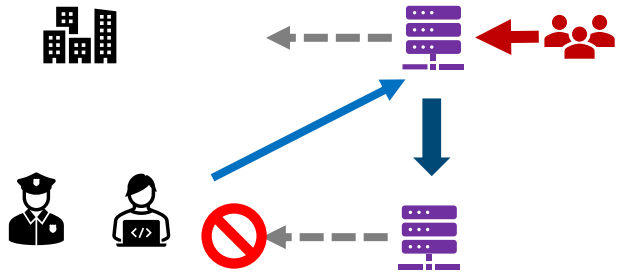
被害組織への報復／攪乱／証拠隠滅

調査妨害、報復、「罠」を仕掛ける

攻撃の「準備段階」を捕捉できた場合

・そもそも国内の組織への攻撃に使われるのかどうかは不明
・ただし、過去に攻撃を行ったアクターが準備したものと判定できる状況

・ドメインテイクダウン／差止
・（即応的な）通信遮断やフィルタリングの準備
・直接操作による無効化



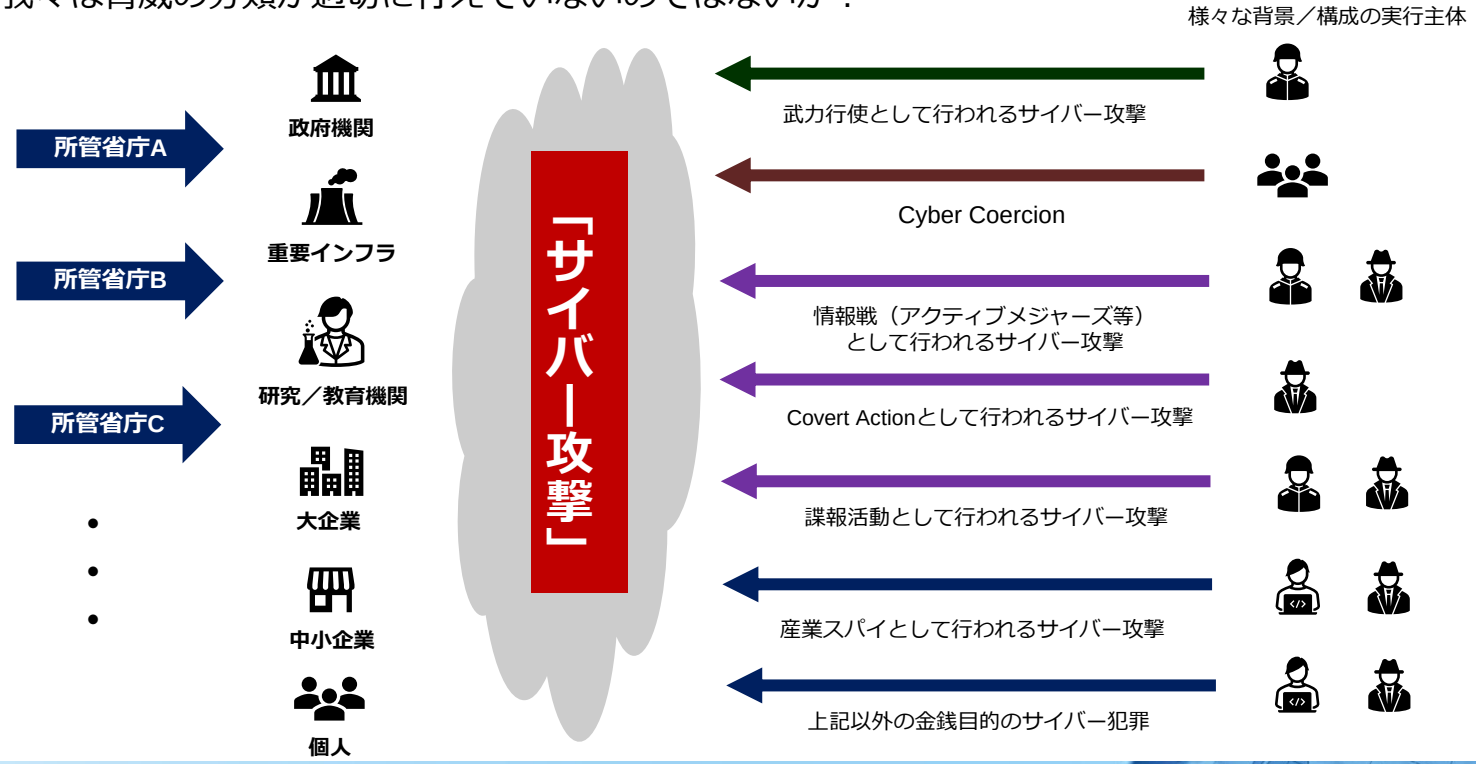
攻撃側はどう出るか

・正規サーバ改ざんやボットネットの多用
・標的国内の正規インフラの乗っ取り／不正使用へ
・「おとり」攻撃インフラへの誘導

プロファイリングの重要性について

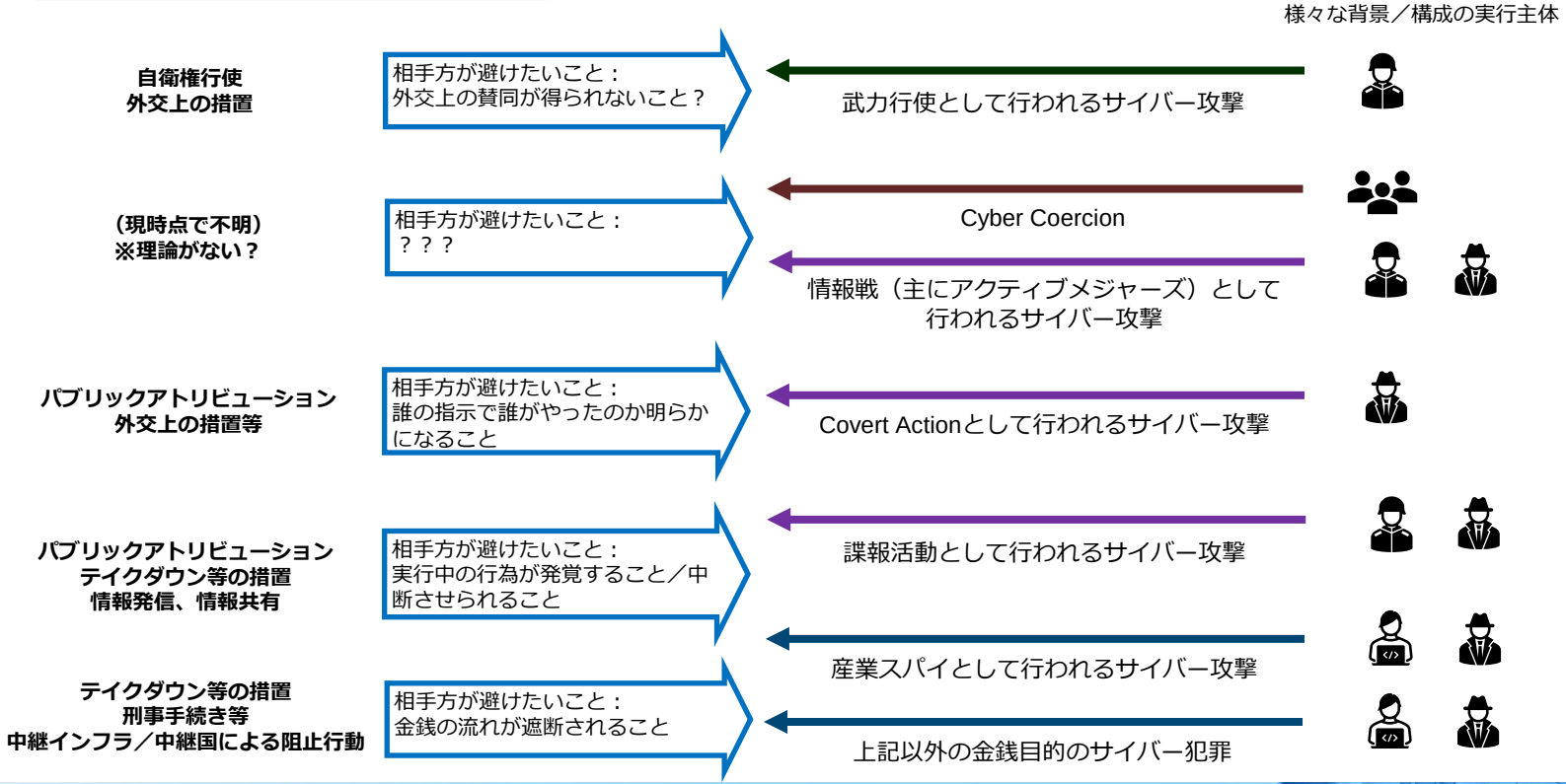
論点：脅威を正しく捉えていない恐れ

- 全く異なる目的／実行主体の様々な攻撃活動をすべて「サイバー攻撃」と表現し、基本的に被害を受ける業種／分野別の対処を行っている
- そもそも我々は脅威の分類が適切に行えていないのではないか？



論点：脅威の特性に応じた有効な対抗措置

- 攻撃の目的／実施主体に応じて、有効な対抗措置は異なる
- **攻撃者のプロファイリングが重要**



先行事例から

（プロ）アクティブなオペレーションの海外事例

- **ソフトな事例**
  - 2014年Sony Picture Entertainment事案における（結果として）速やかな情報共有／公表
  - 2022年ウクライナ侵攻前における複数のワイパー事案に関する早期の情報共有／公表
- **（比較的）ソフトな事例**
  - 2018年米中間選挙前における、Microsoft社におけるAPT28関連ドメインに対する民事差止手続きを用いたテイクダウン
- **ハードな事例**

  ※技術的な効果（の検証状況）は不明
  - 2018年中間選挙前における、米サイバー軍による、ロシアIRAのインフラに対するサイバー作戦（詳細は不明）
  - 2019年 ホルムズ海峡タンカー攻撃事件への報復として攻撃に関わったとするサイバー攻撃グループのインフラに対する米サイバー軍による作戦（詳細は不明）
  - 2020年 Trickbotテイクダウンオペレーションと米サイバー軍による作戦（詳細は不明）

2020年10月 Trickbotへの対抗オペレーションへの評価

KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Report: U.S. Cyber Command Behind Trickbot Tricks

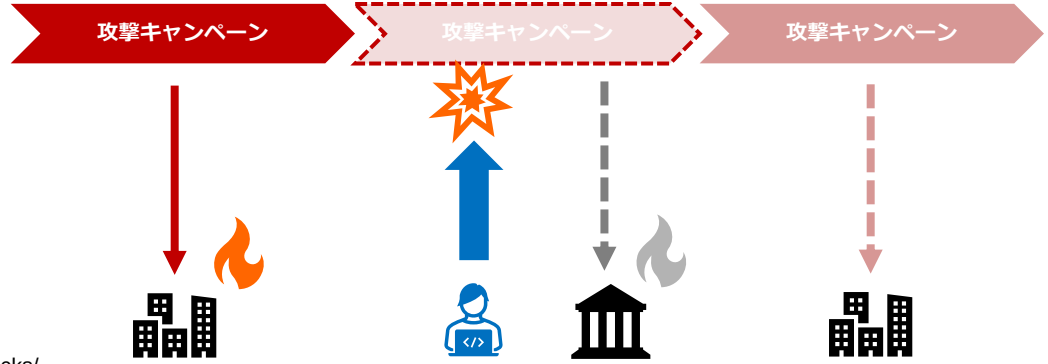
October 10, 2020 55 Comments

A week ago, KrebsOnSecurity broke the news that someone was attempting to disrupt the **Trickbot botnet**, a malware crime machine that has infected millions of computers and is often used to spread ransomware. A new report Friday says the coordinated attack was part of an operation carried out by the U.S. military's **Cyber Command**.

Image: Shutterstock.

On October 2, KrebsOnSecurity reported that twice in the preceding ten days, an unknown entity that had inside access to the Trickbot botnet sent all infected systems a command telling them to disconnect themselves from the Internet servers the Trickbot overlords used to control compromised **Microsoft Windows** computers.

- Microsoftによるドメイン差止手続きの実施
- 加えて、米サイバー軍による「攪乱」作戦が行われた可能性の指摘
- 一連の対応実施後もTrickbotが完全に活動を停止しなかったことから、米サイバー軍の作戦に対しては否定的な見方が相次いだ
- 一方で、この対応は2020年11月の米大統領選挙への事前対応として行われたものであり、当該期間中に大統領選に影響があるような大規模攻撃に悪用されなかったことを評価する見方もある

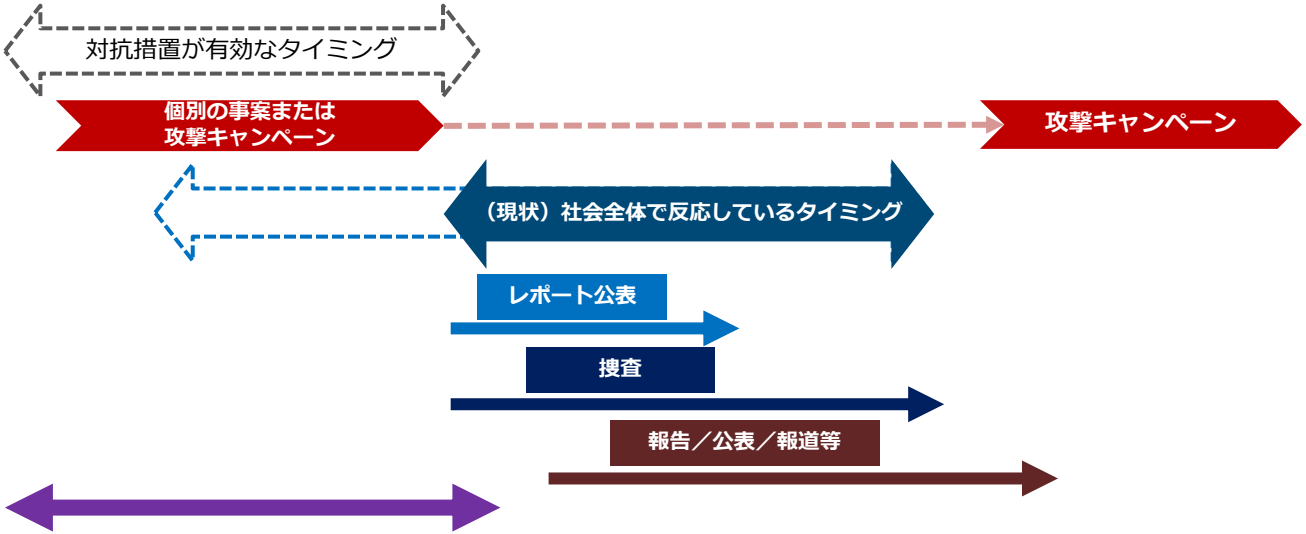


https://krebsonsecurity.com/2020/10/report-u-s-cyber-command-behind-trickbot-tricks/

検討すべきさらなる課題

課題：端緒となる情報の入手方法を考え直す必要性

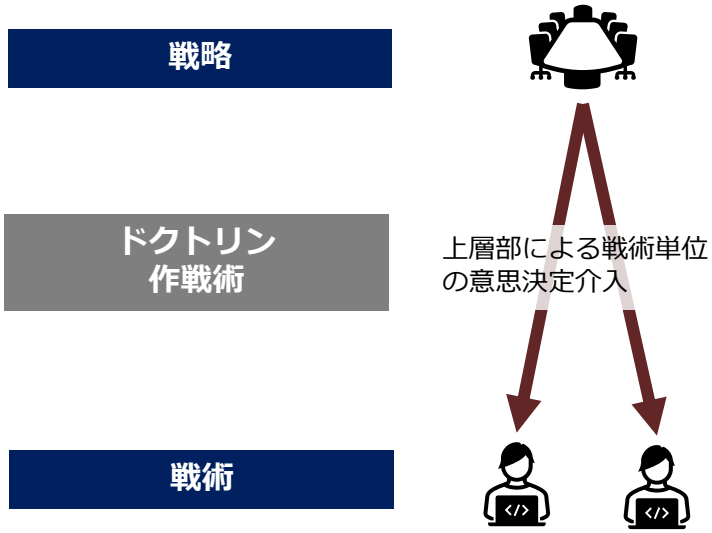
- 早期であればあるほど、対抗措置のオプションは増える
- 単独組織（セキュリティベンダ、専門機関、警察等）だけで対抗措置を検討・実施することはできない
- 個別の組織単位で早期に認知されていても、関係組織間に共有されるまでに時間／調整コストがかかれば、対抗措置検討に必要な時間が消耗されてしまう
- 「被害組織にフォーカスした情報収集」の限界



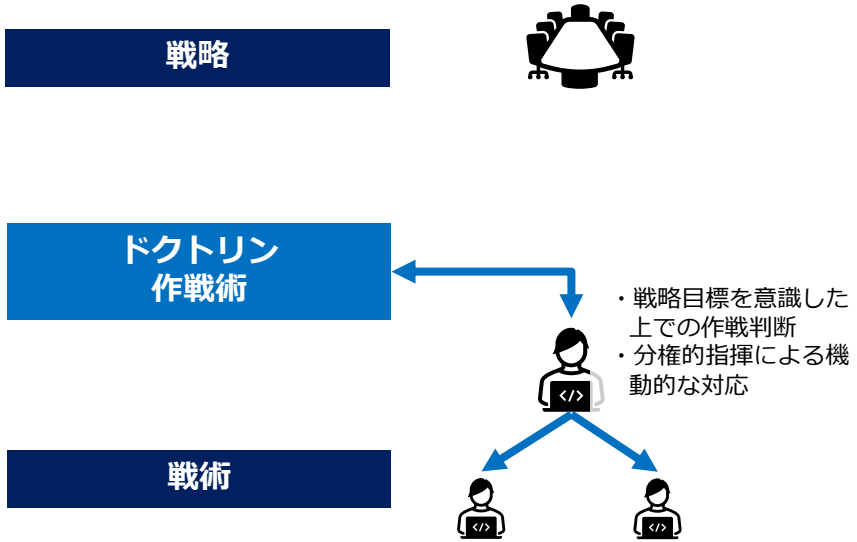
課題：誰が判断して行うのか

- 戦略決定レイヤーが現場の細々した戦術単位の意志決定に口出ししてはいけない
- 各部隊／指揮官はドクトリンを元に、目的に必要な戦術を選ぶ
- 機動性確保のためには分権的指揮が必要になる ← それに耐えうるだけの人材確保が必要

作戦が失敗する典型例



「作戦術」が目指すもの



課題：専門組織やアナリストの活動への影響

各論点に共通するのは「攻撃者の的確なプロファイリングが必須」という点であり、専門組織、アナリストの活動の重要性は一層増す

従前の活動との関係

- “攻撃的”な対抗手段が行われた後の、攻撃側からの報復や妨害にどう対応できるのか？そもそもどのように想定したらいいのか？
- 妨害的オペレーション後にAPTグループの追跡性が下がることをどう受容するか
- 従前のような自主性のある各アナリスト、各セキュリティ企業、研究者単位での情報発信に何らかの制限が及ばないか

新たに求められる役割

- 積極的なオペレーションが行われた後の「評価」を誰がやるのか、という課題への応答
- 積極的オペレーション実施者以外の外部評価におけるアナリストの役割
- 対抗手段の「倫理性」を常に評価する関係者のひとつとしての役割

まとめ

対抗手段の「ドクトリン」の構築

— 攻撃キャンペーンを対象とした対抗手段（の選択）の組み立て ⇒対抗手段の「５W1H」

— どのタイミングで何の目的のために対抗手段を実行すればよいのか、理論的な整理が必要（既存の抑止理論ではなく、攻撃者コストなどの新たな観点からの検討が必要）

官民間連携の重要性

— 攻撃の早期認知のため、「被害組織からの情報提供」に過度に依存しない、新しい情報把握の取り組みが必要

— 法的な権限が必要なより強力な対抗手段を持つようになり、国の機関の役割が増えるほど、対処「タイミング」の課題がネックとなるため、（手続き的）時間がかかるが強力な措置を発動できる国の機関と、ソフトではあるが機動性の高い民間主体の活動との緊密な連携が必要になる。

先行事例の再評価、ケーススタディ

— 先行しているアメリカですら、試行錯誤があり、また、過去事例の評価（効果測定）すら定まっていない。また、対峙するアクター／背景主体も異なる。⇒単に「海外と同じこと」を真似ようとしても意味がない

— 具体的な過去事例のケーススタディに基づいた、技術的／オペレーショナルな各課題の検討が必要

プロファイリング、追跡、評価

— 自国を狙うアクターの正確なプロファイリングがまず必要であり、アナリストの役割はさらに重要になる。

— 積極的オペレーションの結果、特に中長期的影響を評価していくためには、オペレーション実施組織の「外」からのアナリストの追跡／評価が求められるのではないか

さいごに・・・

https://www.hanmoto.com/bd/isbn/9784890634309#

- 「1950年代後半のアメリカ大統領ドワイト・アイゼンハワーが残した「計画（Plan）は無意味（useless）だが、計画立案（Planning）は極めて重要（essential）が」との言葉が含蓄に富む。彼が指摘しているのは、作成された戦略そのものよりも、戦略ができあがるまでの立案プロセスが重要だということである。（同書 p42）
- 「戦略文書を策定する場合には、秘密保全の観点から参加者を限定することがしばしばある。ところが、これまでに述べてきた観点から言えば、そうしたやり方は望ましくない。組織を構成する下位組織が当事者意識を持たなければ、限られたメンバーが作成した戦略文書について**「自分たちの戦略」という意識を持つことはないからである**」（同書 p49）
- 上位戦略が暗黙知として共有されている例
  - 冷戦期アメリカの「封じ込め戦略」は、ジョージ・ケナンの「長電報」や「X論文」はあるが、公式の戦略文書としては定められていない
  - 政権間／政策決定者間で既に「暗黙知」として内面化されていたので、わざわざ文書化する必要がなかった

ご清聴ありがとうございました